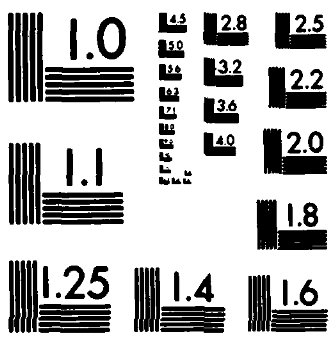
AD-A172 190 THE PMC SYSTEM LEVEL FAULT MODEL: CARDINALITY PROPERTIES OF THE IMPLIED F..(U) JOHNS HOPKINS UNIV BALTIMORE MD DEPT OF ELECTRICAL ENGINEERIN.. 1/1

UNCLASSIFIED M A KENNEDY ET AL. 05 SEP 86 JHU/EECS-86/09 F/G 9/2 NL


1.0
4.5
5.0
5.6
2.8
2.5
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

ersity

(8) (8)

AD-A172 190

THE PMC SYSTEM LEVEL FAULT MODEL:

CARDINALITY PROPERTIES OF THE IMPLIED FAULTY SETS

Mary Ann Kennedy and Gerard G. L. Meyer

REPORT JHU/EECS-86/09

ELECTRICAL ENGINEERING & COMPUTER SCIENCE

86 9 22 051

86 9 22 05

(8)

THE PMC SYSTEM LEVEL FAULT MODEL: CARDINALITY PROPERTIES OF THE IMPLIED FAULTY SETS

Mary Ann Kennedy and Gerard G. L. Meyer

REPORT JHU/EECS-86/09

Electrical Engineering and Computer Science Department

The Johns Hopkins University

Baltimore, Maryland 21218

This work was supported by the Air Force Office of Scientific Research under Contract AFOSR-85-0097.

ABSTRACT

In this paper, we consider one aspect of the PMC system level fault model, the properties of the implied faulty sets. For τ-diagnosable systems that have at most τ faulty units, we present lower bounds on the cardinality of the maximal implied faulty sets. When $\tau \leq 2$, we show that the cardinality of the maximal implied faulty sets is greater than τ. In the case $\tau > 2$ we have two results:

(i) the cardinality of the maximal implied faulty sets associated with the faulty units is greater than or equal to $\tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$, and

(ii) the cardinality of the maximal implied faulty sets of all the units is greater than or equal to $\tau - k + 1$, where now k is the smallest integer such that $\tau \leq 7k + 2$.

Finally, we show that these bounds are greatest lower bounds and in the conclusion indicate how these results may be used in diagnosis algorithms.

I. INTRODUCTION

The PMC system level fault model [PRE67] consists of a set of units $U = \{u_1, u_2, \ldots, u_n\}$ capable of testing one another and a set of ordered pairs $\{(u_i, u_j) \mid u_i \text{ tests } u_j\}$ describing the organization of the tests. The model is defined by the fault-test relationship which specifies the test outcome $a_{i,j}$ in terms of the status of both the unit u_i applying the test and the unit u_j being tested. If u_i is nonfaulty, then $a_{i,j} = 0$ if u_j is nonfaulty and $a_{i,j} = 1$ if u_j is faulty, and if u_i is faulty, the test outcome $a_{i,j} = 0$ or 1, independent of the status of u_j. A collection of all test outcomes is called a syndrome. The model can be represented by the directed graph $G = (U,E)$, in which the vertices in U are the units and the edges in E are the tests between units. The test outcomes are the edge labels of the graph, and thus G has both 0-edges and 1-edges. The model has been studied extensively and among topics that have been addressed are conditions for t-diagnosability ([PRE67], [HAK74], [ALL75], [CHW81], [KEN84]) and algorithms for system diagnosis ([KAM75], [MEY78], [MAD77], [MEY81], [DAH84], [DAH85]). In this paper we consider only system diagnosis, and more specifically those properties of implied faulty sets that may be used for system diagnosis.

Given a syndrome, the diagnosis problem consists of identifying the set of faulty units F_S and the set of nonfaulty units G_S. A system is t-diagnosable if and only if all faulty units can be identified from the syndrome whenever the system has at most t faulty units [PRE67]. For a given syndrome, a partition (G,F) is consistent with the syndrome if

every test among units in G has a 0 outcome and every test from a unit in G to a unit in F has a 1 outcome. Diagnosis of a τ-diagnosable system with at most τ faulty units requires identifying the unique consistent partition (G_S, F_S) such that $|F_S| \leq \tau$.

Diagnosis algorithms use the concepts of implied nonfaulty and implied faulty sets either directly [MEY79], [MEY81], [DAH85], or indirectly to transform the diagnosis problem into a graph support problem [MAD77], [DAH84]. We recall that for a given syndrome, the implied nonfaulty set $G(u_i)$ for the unit u_i is the set of all units that are implied nonfaulty if u_i is assumed to be nonfaulty and the implied faulty set $L(u_i)$ is the set of all units that are implied faulty if u_i is assumed to be nonfaulty [KAM75]. Thus, if we define a *0-path* in the graph G as a path in which every edge is a 0-edge, we see that

$$G(u_i) = \{u_i\} \cup \{u_j \mid \textit{there is a 0-path from } u_i \textit{ to } u_j\} ,$$

and

$$L(u_i) = \{u_j \mid \textit{there exists } u_p \textit{ in } G(u_i),\ u_q \textit{ in } G(u_j) \textit{ and either } a_{p,q} = 1 \textit{ or } a_{q,p} = 1 \textit{ or both}\} .$$

It is clear that if $L(u_i) \cap G(u_i) \neq \phi$, then the unit u_i is faulty. Many diagnosis algorithms take advantage of this fact by declaring such units faulty and concentrating on the problem of diagnosing the resulting reduced system. Direct algorithms are less complex than graph support algorithms, but the needed properties of implied sets are known only for restricted classes of testing structures. For example, if a system is

τ-diagnosable and has at most τ faulty units, the algorithm in [MEY81] identifies the set of faulty units if there exists at least one faulty unit u_i such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau + 1$. Only τ-diagnosable systems in which no two units test each other are known to have this property [MEY83]. The structural constraints associated with self-implicating systems [DAH85] are even stronger.

In this paper we do not impose structural constraints on the test organization, and we analyze the properties of the implied faulty sets that may be used in direct diagnosis algorithms only under the assumptions that the system is τ-diagnosable and that the number of faulty units is not greater than τ. The main thrust of our effort is directed at obtaining lower bounds on the cardinality of the maximal implied faulty sets associated with not only the units in F_S, but also the units in G_S. When $\tau \leq 2$, a direct approach is possible and the cardinality of the maximal implied faulty sets is greater than τ. This result is presented in Section II. When $\tau > 2$, we need the concept of a critical subset in order to pursue our investigation. A subset X of S is a critical subset of S if and only if there are no 0-edges from $S - X$ into X. Critical subsets and partitions of critical subsets play a major role in the analysis of implied faulty sets when $\tau > 2$, and their properties are discussed in Section III. The set F_S of faulty units is a critical subset of S, and under the appropriate assumptions, its partition consists of either one or two blocks. That fact is used in Section IV to obtain the greatest lower bound on the cardinality of the maximal sets $L(u_i)$ associated with the units in F_S, that is at least one unit u_i in F_S

exists such that $|L(u_i)| \geq \tau-k+1$, where k is the smallest integer such that $\tau \leq 6k+2$. When $\tau > 2$, the unit with the maximal implied faulty set may not be faulty, and thus we must consider not only the units in F_S, but also the nonfaulty units. This analysis is presented in Section V. In that case, we note that, under the appropriate assumptions, we may have one, two or three blocks in the partition of F_S. The analysis is more complex than when we restrict ourselves to only faulty units, but we are again able to obtain the greatest lower bound on the cardinality of the maximal $L(u_i)$, that is at least one unit u_i in S exists such that $|L(u_i)| \geq \tau-k+1$, where k is the smallest integer such that $\tau \leq 7k+2$. Finally, in Section VI, we indicate briefly how the paper's results may be used in decoding algorithms.

II. IMPLIED FAULTY SETS: $\tau \leq 2$

Theorem 1: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if $\tau \leq 2$, at least one unit u_i in F_S exists such that $|L(u_i)| \geq \tau + 1$.

Proof: Suppose that S is τ-diagnosable, $\tau \leq 2$, and $F_S = \{u_j\}$. The faulty unit u_j is tested by a minimum of τ nonfaulty units. Every unit that tests u_j implies it faulty, hence is in $L(u_j)$. If u_j is tested by more than τ other units, then $|L(u_j)| \geq \tau + 1$. Suppose that u_j is tested by exactly τ other units, and let $Z = \{u_j\} \cup \{u_k \mid u_k \text{ tests } u_j\}$. Since S is τ-diagnosable and $|Z| = \tau + 1 \leq 2\tau$ for $\tau \geq 1$, Z must be tested by at least

$$\tau - \lceil(\tau+1)/2\rceil + 1 = \lfloor(\tau+1)/2\rfloor$$

other units in $S - Z$. All units in $S - Z$ are nonfaulty, so every unit in $S - Z$ that tests Z belongs to $L(u_j)$, and therefore $|L(u_j)| \geq \tau + \lfloor(\tau+1)/2\rfloor \geq \tau + 1$ for $\tau \geq 1$.

Suppose now that S is τ-diagnosable, $\tau = 2$, and $F_S = \{u_j, u_k\}$. If either u_j or u_k is tested by more than τ nonfaulty units then either $|L(u_j)| \geq \tau + 1$ or $|L(u_k)| \geq \tau + 1$ or both. Suppose that each of $\{u_j, u_k\}$ is tested by at most τ nonfaulty units. Let X be the set of units in $S - F_S$ that test either u_j or u_k. At least τ nonfaulty units test either one or both of the units in F_S, hence $|X| \geq 2$. If $|X| = 2$, then $|X| + |F_S| = 4 = 2\tau$ and at least $\tau - \lceil 2\tau/2\rceil + 1 = 1$ unit in $S - (F_S \cup X)$ must test the units in $X \cup F_S$. Let Y be the set of units in $S - (X \cup F_S)$ that test the units in $X \cup F_S$, then

$|X| + |Y| \geq 3 = \tau + 1$. All units in Y are nonfaulty, thus $(X \cup Y) \subseteq (L(u_j) \cup L(u_k))$. This implies that either $|L(u_j) \cap (X \cup Y)| \geq 2$ or $|L(u_k) \cap (X \cup Y)| \geq 2$ or both.

Now consider the tests between the faulty units u_j and u_k. If u_j tests u_k and $a_{j,k} = 0$ then $L(u_k) \subseteq L(u_j)$, $(X \cup Y) \subseteq L(u_j)$, and $|L(u_j)| \geq \tau + 1$. Similarly, if u_k tests u_j and $a_{k,j} = 0$ then $(X \cup Y) \subseteq L(u_k)$ and $|L(u_k)| \geq \tau + 1$. If u_j tests u_k and $a_{j,k} = 1$ or if u_k tests u_j and $a_{k,j} = 1$ then u_j is in $L(u_k)$ and u_k is in $L(u_j)$. In this case $|L(u_j)| \geq 1 + |L(u_j) \cap (X \cup Y)|$ and $|L(u_k)| \geq 1 + |L(u_k) \cap (X \cup Y)|$, thus either $|L(u_j)| \geq \tau + 1$ or $|L(u_k)| \geq \tau + 1$ or both.

If there are no tests between u_j and u_k then both u_j and u_k are tested by exactly τ nonfaulty units. Let $\{u_p, u_q\}$ be the nonfaulty units that test u_j, thus $\{u_p, u_q\} \subseteq L(u_j)$. Since S is τ-diagnosable, at least τ other units test the pair $\{u_j, u_p\}$. Only one unit, u_q, is known to test this pair. If a nonfaulty unit other than u_q tests either u_j or u_p, then this unit also belongs to $L(u_j)$ and $|L(u_j)| \geq \tau + 1$. If u_k tests u_p and $a_{k,p} = 0$, then u_k is in $L(u_j)$ and $|L(u_j)| \geq \tau + 1$. Therefore, u_k must test u_p and $a_{k,p} = 1$. A similar situation occurs for the pair $\{u_j, u_q\}$, therefore, u_k tests u_q, $a_{k,q} = 1$, and $\{u_p, u_q\} \subseteq L(u_k)$. The set $Z = \{u_j, u_k, u_p, u_q\}$ has cardinality $|Z| = 4 = 2\tau$, so Z must be tested by at least one nonfaulty unit in $S - Z$. Any nonfaulty unit that tests a unit in Z belongs to either $L(u_j)$ or $L(u_k)$ or both, thus either $|L(u_j)| \geq \tau + 1$ or $|L(u_k)| \geq \tau + 1$ or both. $\square$

Theorem 1 shows that for τ-diagnosable systems in which $1 \leq |F_S| \leq \tau \leq 2$ at least one faulty unit u_i exists such that $|L(u_i)| \geq \tau + 1$. The next result shows that for the implied faulty sets associated with faulty units this lower bound is actually the greatest lower bound.

Lemma 1: To the integers $\tau = 1$ and $\tau = 2$ correspond at least one τ-diagnosable system S that has τ faulty units and one syndrome such that:
(i) $L(u_i) \cap G(u_i) = \phi$ for every unit u_i in S,
(ii) $|L(u_i)| = \tau + 1$ for every faulty unit u_i, and
(iii) $|L(u_i)| = \tau$ for every nonfaulty unit u_i.

Proof: The examples in this proof are from the class of $D_{\delta,\tau}$ τ-diagnosable systems [PRE67]. Figure 1 shows a 1-diagnosable $D_{1,1}$ system consisting of three units: unit u_1 is faulty and units u_2 and u_3 are nonfaulty. For the given syndrome the implied nonfaulty sets are $G(u_1) = \{u_1\}$, $G(u_2) = \{u_2,u_3\}$, and $G(u_3) = \{u_3\}$. The implied nonfaulty sets are $L(u_1) = \{u_2,u_3\}$, $L(u_2) = \{u_1\}$, and $L(u_3) = \{u_1\}$. The system is 1-diagnosable, it has 1 faulty unit, it has a syndrome such that $L(u_i) \cap G(u_i) = \phi$ for all units u_i, $|L(u_1)| = 2$ for the faulty unit u_1, and $|L(u_i)| = 1$ for the nonfaulty units u_2 and u_3.

Figure 2 shows a 2-diagnosable $D_{1,2}$ system that has five units. The units $\{u_1,u_2\}$ are faulty and the units $\{u_3,u_4,u_5\}$ are nonfaulty. For the given syndrome the implied nonfaulty sets are $G(u_1) = \{u_1,u_2\}$, $G(u_2) = \{u_2\}$, $G(u_3) = \{u_3,u_4,u_5\}$, $G(u_4) = \{u_4,u_5\}$, and $G(u_5) = \{u_5\}$. The implied faulty sets are $L(u_i) = \{u_3,u_4,u_5\}$, $i = 1$ and 2, and

$L(u_i) = \{u_1, u_2\}$, i = 3, 4 and 5. The system is 2-diagnosable, it has 2 faulty units, it has a syndrome such that $L(u_i) \cap G(u_i) = \phi$ for all units u_i, $\|L(u_i)\| = 3$ for the two faulty units, and $\|L(u_i)\| = 2$ for the three nonfaulty units.

In both examples the τ-diagnosable system has τ faulty units and a syndrome such that $L(u_i) \cap G(u_i) = \phi$ for all units u_i, $\|L(u_i)\| = \tau + 1$ for all of the faulty units, and $\|L(u_i)\| = \tau$ for all of the nonfaulty units. □

Theorem 1 gives a lower bound on the cardinality of the maximal implied faulty set associated with the faulty units. It is clear that $\|L(u_i)\| \leq \tau$ whenever the unit u_i in nonfaulty, and therefore when $\tau \leq 2$, the consideration of nonfaulty units does not result in an improvement of the lower bound on the cardinality of $L(u_i)$.

Theorem 2: If S is τ-diagnosable, if $1 \leq \|F_S\| \leq \tau$, and if $\tau \leq 2$, at least one unit u_i in S exists such that $\|L(u_i)\| \geq \tau + 1$.

III. CRITICAL SUBSETS

A subset X of S is a critical subset of S if and only if there are no 0-edges from $S - X$ into X or equivalently:

Definition 1: A subset X of S is a *critical subset* of S if and only if $G(u_i) \cap X = \phi$ for all units u_i in $S - X$.

Critical subsets play a major role in the investigation of the properties of the PMC system level fault model because the set of faulty units F_S is always a critical subset of S. Thus to be a critical subset of S is a necessary condition for a subset X to be the set of faulty units, but that condition is not sufficient. Note that Definition 1 implies that the empty set ϕ and the set S itself are both critical subsets of S.

If S is τ-diagnosable the next result gives a lower bound on the cardinality of the maximal implied faulty set for units in critical subsets.

Lemma 2: If S is τ-diagnosable and if X is a non-empty critical subset of S, then $|L(u_*)| \geq \tau - \lceil |X|/2 \rceil + 1$ for at least one unit u_* in X.

Proof: The set X is a critical subset of S and therefore there are no 0-edges from $S - X$ to X. Let u_* be a unit in X such that $|L(u_*)| \geq |L(u_j)|$ for all u_j in X and let X' be the subset of X that consists of all the units u_j for which u_* is in $G(u_j)$. The set X' contains u_* and all units that imply u_* nonfaulty, and consequently $|X'| \leq |X|$, there are no 0-edges from $S - X'$ to X', and $L(u_*) \subseteq L(u_j)$

for all u_j in X'. By definition, however, $|L(u_*)| \geq |L(u_j)|$ for all u_j in X', thus $L(u_j) = L(u_*)$ for all u_j in X'. Every edge from $S - X'$ to X' is a 1-edge, therefore every unit in $S - X'$ that tests X' belongs to $L(u_*)$. S is τ-diagnosable, so at least $\tau - \lceil |X'|/2 \rceil + 1$ units in $S - X'$ test the units in X'. Therefore,

$$|L(u_*)| \geq \tau - \lceil |X'|/2 \rceil + 1 \geq \tau - \lceil |X|/2 \rceil + 1$$

for at least one unit u_* in X. □

We know that F_S is a critical set. If in addition S is τ-diagnosable, has at most τ faulty units, and there exists a faulty unit that implies every unit in F_S nonfaulty, then either this unit implies itself faulty, or the cardinality of the implied faulty set of this unit is bounded from below by $\tau + 1$ or both.

Lemma 3: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if a unit u_* in F_S exists such that $G(u_*) \cap F_S = F_S$, then either $G(u_*) \cap L(u_*) \neq \phi$ or $|L(u_*)| \geq \tau + 1$.

Proof: Suppose that S is τ-diagnosable, $1 \leq |F_S| \leq \tau$, there exists a unit u_* in F_S such that $G(u_*) \cap F_S = F_S$, and $G(u_*) \cap L(u_*) = \phi$. All edges among units in $(G(u_*) \cap F_S)$ are 0-edges, all edges from $(G(u_*) \cap F_S)$ to $L(u_*)$ are 1-edges, and all units in the sets $L(u_*)$ and $N(u_*) = S - (L(u_*) \cup G(u_*))$ are nonfaulty.

There are no tests from units in $N(u_*)$ to units in either $(G(u_*) \cap F_S)$ or $L(u_*)$, nor are there any tests from units in $(G(u_*) \cap G_S)$ to units in either $(G(u_*) \cap F_S)$ or $L(u_*)$. There are also

no tests from $G(u_*)$ to $N(u_*)$. Thus, the partition

$$(G_1,F_1) = ((G(u_*) \cup N(u_*), L(u_*))$$

is a consistent partition of S (see Figure 3). If $|F_1| = |L(u_*)| \leq \tau$, then S has two consistent partitions, (G_S,F_S) and (G_1,F_1), such that $|F_S| \leq \tau$ and $|F_1| \leq \tau$, and hence S can not be τ-diagnosable. Thus, if S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if there exists a unit u_* in F_S such that $(G(u_*) \cap F_S) = F_S$, then either $L(u_*) \cap G(u_*) \neq \phi$ or $|L(u_*)| \geq \tau + 1$. □

Let X be a critical subset of S. By definition u_i is in $G(u_i)$, and thus if u_i is in X, it is in $G(u_i) \cap X$ and $G(u_i) \cap X$ is non-empty. If u_i is not in X, then we know that $G(u_i) \cap X$ is empty. We may then conclude that a unit u_i is in a critical set X if and only if $G(u_i) \cap X \neq \phi$. That characteristic property of critical subsets is used by the following algorithm to generate partitions of the critical subsets of S.

Algorithm 1: Let X be a critical subset of S.

Step 1: Let $i = 1$ and let $\hat{X} = \phi$.

Step 2: Find a unit u_{i*} in $X - \hat{X}$ such that $|G(u_{i*}) \cap (X - \hat{X})| \geq |G(u_j) \cap (X - \hat{X})|$ for all units u_j in $X - \hat{X}$, and let $X_i = G(u_{i*}) \cap (X - \hat{X})$.

Step 3: Let $\hat{X} = \hat{X} \cup X_i$.

Step 4: If $X - \hat{X} = \phi$, stop; otherwise let $i = i + 1$ and go to Step 2.

If X is a critical subset of S, if $\{X_1,X_2,\ldots,X_p\}$ is a partition of X generated by Algorithm 1, and if for each i in $\{1,2,\ldots,p\}$, we let $|X_i| = x_i$, then:

(i) $x_i \geq x_j$ and there are no 0-edges from X_i to X_j whenever $i < j$,

(ii) $G(u_{i*}) \cap X_i = X_i$ for all i in $\{1,2,\ldots,p\}$,

(iii) $L(u_j) \subset L(u_{i*})$ for all u_j in X_i, and

(iv) the last block X_p is a critical subset of S.

To each block X_i of a partition generated by Algorithm 1, let us associate a subset $\tilde{X}_i$ that contains u_{i*} and all units that imply u_{i*} nonfaulty, that is

$$\tilde{X}_i = \{u_{i*}\} \cup \{u_j \mid u_{i*} \text{ is in } G(u_j)\} \ .$$

Thus, if u_{i*} is implied faulty, all units in $\tilde{X}_i$ are implied faulty, and if $j > i$, there are no 0-edges from X_j to $\tilde{X}_i$, otherwise u_{i*} would be in $G(u_{j*})$.

If S is τ-diagnosable and if X is a critical subset of S, Lemma 2 gives a lower bound for the maximal $L(u_i)$, u_i in X. If at most τ units in S are faulty and $|L(u_i)|$ is bounded from above, then any partition of a critical subset generated by Algorithm 1 has the following properties;

Lemma 4: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, if X is a critical subset of S, if $\{X_1,X_2,\ldots,X_p\}$ is a partition of X generated by Algorithm 1, if $|L(u_i)| \leq \tau - k$ for all units u_i in S, where $k \leq \lceil |X|/2 \rceil - 1$, and

if j is the unique integer satisfying $j(2k+1) \leq |X| < (j+1)(2k+1)$, then $|\tilde{X}_i| \geq 2k + 1$ for all i in $\{1,2,\ldots,p\}$, $|X| \geq p(2k + 1)$, and $p \leq j$.

Proof: Suppose that S is τ-diagnosable, $|F_S| \leq \tau$, X is a critical subset of S, and $|L(u_i)| \leq \tau - k$ for all units u_i in S, where $k \leq \lceil |X|/2 \rceil - 1$. Let $\{X_1,X_2,\ldots,X_p\}$ be a partition of X generated by Algorithm 1. There are no 0-edges from $S - \tilde{X}_i$ to $\tilde{X}_i$ for i in $\{1,2,\ldots,p\}$. Lemma 2 implies that there exists at least one unit u_j in $\tilde{X}_i$ such that $|L(u_j)| \geq \tau - \lceil \tilde{x}_i/2 \rceil + 1$, where $\tilde{x}_i = |\tilde{X}_i|$. But $|L(u_j)| \leq \tau - k$ for all u_j in X, thus $\tilde{x}_i \geq 2k + 1$, and from the fact that $|X| = \sum_{i=1}^{p} |X_i|$ and $|X_i| \geq \tilde{x}_i$ for all i in $\{1,2,\ldots,p\}$ we may conclude that $|X| \geq p(2k + 1)$. We have shown that $(j+1)(2k+1) > |X| \geq p(2k+1)$, therefore $j+1 > p$ and $j \geq p$. □

IV. IMPLIED FAULTY SETS OF FAULTY UNITS: $\tau > 2$

The set of faulty units, F_S, is a critical subset and as a result of our assumptions on τ and the maximal $|L(u_i)|$, we will see that Algorithm 1 generates a partition of F_S consisting of one or two blocks. Lemma 3 deals with the case of a single block and Lemma 5 below handles the two block case. Using these two results, Theorem 3 presents a lower bound on the maximal implied faulty sets associated with the faulty units. Lemma 6 then shows that this bound is a greatest lower bound.

Lemma 5: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, if $\tau > 2$, and if Algorithm 1 generates a two block partition $\{X_1, X_2\}$ of F_S, at least one unit u_i in F_S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$.

Proof: Suppose that the following assumptions are satisfied:

(H1) S is τ-diagnosable,

(H2) $\tau > 2$,

(H3) $1 \leq |F_S| \leq \tau$,

(H4) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, and

(H5) $|L(u_i)| \leq \tau - k$ for all u_i in F_S, where k is the smallest integer such that $\tau \leq 6k + 2$.

(H6) Algorithm 1 generates a partition $\{X_1, X_2\}$ of F_S.

The partition of F_S consists of two blocks, hence Lemma 4 implies that $|F_S| \geq 2(2k + 1)$, and thus (H1) through (H5) can be true only when $\tau \geq |F_S| \geq 4k + 2$.

There exist units u_{1*} and u_{2*} in X_1 and X_2, respectively, such that $G(u_{1*}) \cap X_1 = X_1$ and $G(u_{2*}) \cap X_2 = X_2$. Thus, $L(u_i) \subseteq L(u_{1*})$ for all u_i in X_1 and $L(u_i) \subseteq L(u_{2*})$ for all u_i in X_2. Now let

$$A = (L(u_{1*}) \cap L(u_{2*})) \cap G_S,$$

$$B_1 = (L(u_{1*}) \cap G_S) - A,$$

$$B_2 = (L(u_{2*}) \cap G_S) - A,$$

$$Z = X_1 \cup X_2 \cup A \cup B_1 \cup B_2,$$

and let $|A| = a$, and $|B_i| = b_i$ for i in $\{1,2\}$.

The set $S - Z$ contains only nonfaulty units, and since

$$A \cup B_1 \cup B_2 = (L(u_{1*}) \cup L(u_{2*})) \cap G_S$$

there are no tests from $S - Z$ to Z. Thus Z itself must be τ-diagnosable, therefore

$$|Z| = x_1 + x_2 + a + b_1 + b_2 \geq 2\tau + 1$$

and since $x_1 + x_2 \leq \tau$ and both Z and S are τ-diagnosable, we see that

$$a + b_1 + b_2 \geq \tau + 1 \ . \qquad (1)$$

Let $W_1 = L(u_{2*}) \cap X_1$ and let $W_2 = L(u_{1*}) \cap X_2$, also let $w_1 = |W_1|$ and $w_2 = |W_2|$. If u_{1*} is not implied faulty by u_{2*}, then $W_1 = W_2 = \phi$. If u_{1*} is in $L(u_{2*})$, then $\tilde{X}_1 \subseteq W_1 \subseteq X_1$ and $\tilde{X}_2 \subseteq W_2 \subseteq X_2$, where $\tilde{X}_i$

contains u_{i*} and all units in X_i that imply u_{i*} nonfaulty, i in $\{1,2\}$.

System Z is shown in Figure 4. We see that $L(u_{1*}) = A \cup B_1 \cup W_2$ and $L(u_{2*}) = A \cup B_2 \cup W_1$. Assumption (H5) implies:

$$\|L(u_{1*})\| = a + b_1 + w_2 \leqslant \tau - k, \tag{2}$$

$$\|L(u_{2*})\| = a + b_2 + w_1 \leqslant \tau - k \,, \tag{3}$$

and thus

$$a + b_1 + b_2 \leqslant 2\tau - 2k - (a + w_1 + w_2) \,. \tag{4}$$

The units in $(X_2 \cup B_2)$ are tested only by the units in $(A \cup W_1)$, so (H1) implies that

$$x_2 + b_2 + 2(a + w_1) \geqslant 2\tau + 1 \,. \tag{5}$$

Substituting Eq. (3) into Eq. (5) we get

$$a + w_1 \geqslant \tau + k + 1 - x_2, \tag{6}$$

and substituting Eq. (6) into Eq. (4) produces

$$a + b_1 + b_2 \leqslant \tau - 3k - 1 + (x_2 - w_2) \,. \tag{7}$$

We know that $x_2 \leqslant x_1$, $x_1 + x_2 \leqslant \tau$, $\tau \leqslant 6k + 2$, and therefore $x_2 \leqslant \lfloor \tau/2 \rfloor \leqslant 3k + 1$. Note that $w_2 \geqslant 0$, thus Eq. (7) becomes

$$a + b_1 + b_2 \leqslant \tau \tag{8}$$

which contradicts Eq. (1).

The assumptions (H1), (H2), (H3), (H4), (H5), and (H6) lead to a contradiction, and we may conclude that if S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, if $\tau > 2$, and if Algorithm 1 generates a two block partition of F_S, at least one unit u_i exists in F_S such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$. □

This result is used in the proof of the following theorem.

Theorem 3: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if $\tau > 2$, at least one unit u_i in F_S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$.

Proof: Suppose the system S satisfies the following assumptions:

(H1) S is τ-diagnosable,

(H2) $\tau > 2$,

(H3) $1 \leq |F_S| \leq \tau$,

(H4) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, and

(H5) $|L(u_i)| \leq \tau - k$ for all u_i in F_S, where k is the smallest integer such that $\tau \leq 6k + 2$.

Let $\{X_1, X_2, \ldots, X_p\}$ be a partition of the critical subset F_S generated by Algorithm 1. Lemma 4 implies that $|F_S| \geq p(2k + 1)$, where p is the number of blocks in the partition. Since $|F_S| \leq \tau \leq 6k + 2$, this implies that $p \leq 3 - (1/(2k+1))$. Both k and p are positive integers, thus $1 \leq p \leq 2$, and we may conclude that any partition of F_S generated by Algorithm 1 has at most two blocks.

If the partition of F_S consists of a single block, then there exists a unit u_{1*} in F_S such that $G(u_{1*}) \cap F_S = F_S$. Lemma 3 implies that either $L(u_{1*}) \cap G(u_{1*}) \neq \phi$ or $|L(u_{1*})| \geq \tau + 1$, contradicting either assumption (H4) or assumption (H5). If the partition of F_S consists of two blocks, then Lemma 5 implies that assumptions (H1), (H2), (H3), (H4), and (H5) lead to a contradiction.
We conclude that if S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if $\tau > 2$, at least one unit u_i exists in F_S such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$. □

Theorems 1 and 3 show that the set of values of τ may be partitioned into intervals of length 6, except for the first interval that is of length 2. For τ-diagnosable systems in which both $1 \leq |F_S| \leq \tau$ and $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, Theorem 1 implies that if $\tau \leq 2$, at least one faulty unit u_i exists such that $|L(u_i)| \geq \tau + 1$, and Theorem 3 implies that if $\tau \leq 8$, at least one faulty unit u_i exists such that $|L(u_i)| \geq \tau$, if $\tau \leq 14$, at least one faulty unit u_i exists such that $|L(u_i)| \geq \tau - 1$, and so forth. The next result shows that for $\tau > 2$ the lower bound given in Theorem 3 is actually the greatest lower bound on the cardinality of the maximal $L(u_i)$ associated with the faulty units.

Lemma 6: To every integer $\tau > 2$ corresponds at least one τ-diagnosable system S that has τ faulty units and one syndrome such that:
(i) $L(u_i) \cap G(u_i) = \phi$ for every unit u_i in S,
(ii) $|L(u_i)| = \tau - k + 1$ for every faulty unit u_i, where k is the

smallest integer such that $\tau \leq 6k + 2$, and

(iii) $|L(u_i)| = \tau$ for at least one nonfaulty unit u_i.

Proof: Choose a value of τ, $\tau > 2$, and find the smallest integer k such that $\tau \leq 6k + 2$. Construct a system S that has the partition $\{A, B_1, B_2, B_3, X_1, X_2, X_3\}$ as shown in Figure 5. The cardinality of each block is as follows: $|A| = \tau - 3k + 1$, $|B_i| = k$, for i in $\{1,2,3\}$, $|X_1| = \tau - 4k + 2$, and $|X_2| = |X_3| = 2k - 1$. Each block in the partition is nonempty and S has cardinality $2\tau + 1$.

The tests among units in the systems are organized in the following manner. The units within each block are completely connected. That is, every unit in X_1 tests every other unit in X_1, every unit in B_2 tests every other unit in B_2, and so forth. The edges between blocks shown in Figure 5 indicate that every unit in the block at the tail of the edge tests every unit in the block at the head of the edge. For example, every unit in X_1 tests every unit in B_1 and vice versa, every unit in A tests every unit in B_2, and so forth.

To show that S is τ-diagnosable we use the approach of Sullivan [SUL84]. We solve n network flow problems, where n is the number of units in the system, to find the maximum τ for which S is τ-diagnosable. For each unit u_i in S construct a flow graph $G_i = (V', E')$ where $V' = U \cup \{s_1\}$ and $E' = E \cup \{(s_1, u_j) | u_j \text{ in } U\}$. In G_i the vertex s_1 is the source and the vertex u_i is the sink. Each vertex, excluding the source and the sink, has capacity 1, each edge in $E \subset E'$ has infinite capacity, and each edge (s_1, u_j) in $(E' - E)$ has capacity 1/2. Since the

system is symmetric we need to solve only seven network flow problems, one for each block. We omit the details of solving the network flow problems and claim that for each of the networks the maximum flow is $(\tau + 1/2)$, and thus S is τ-diagnosable ([SUL84], Theorem 4.1).

The set of nonfaulty units is

$$G_S = A \cup B_1 \cup B_2 \cup B_3 ,$$

the set of faulty units is

$$F_S = X_1 \cup X_2 \cup X_3 ,$$

and $|F_S| = (\tau - 4k + 2) + 2(2k - 1) = \tau$. Figure 5 shows a syndrome consistent with the set of faulty units. For this syndrome the following table lists the implied nonfaulty set, the implied faulty set, and the cardinality of the implied faulty set for each unit in S.

u_i in	$G(u_i)$	$L(u_i)$	$\lvert L(u_i)\rvert$
X_1	X_1	$A \cup B_1 \cup B_3$	$\tau - k + 1$
X_2	X_2	$A \cup B_1 \cup B_2$	$\tau - k + 1$
X_3	X_3	$A \cup B_2 \cup B_3$	$\tau - k + 1$
A	$A \cup B_1 \cup B_2 \cup B_3$	$X_1 \cup X_2 \cup X_3$	τ
B_1	B_1	$X_1 \cup X_2$	$\tau - 2k + 1$
B_2	B_2	$X_2 \cup X_3$	$4k - 2$
B_3	B_3	$X_1 \cup X_3$	$\tau - 2k + 1$

The system S is τ-diagnosable for $\tau > 2$, it has τ faulty units, and

it has a syndrome such that

(i) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S,

(ii) $|L(u_i)| = \tau - k + 1$ for each faulty unit u_i, where k is the smallest integer such that $\tau \leq 6k + 2$, and

(iii) $|L(u_i)| = \tau$ for each nonfaulty unit in A and $A \neq \phi$. □

Lemma 6 shows that the lower bound given in Theorem 3 is the greatest lower bound. It also shows that the unit with the maximal implied faulty set may be nonfaulty. In the next section we improve the lower bound on the cardinality of the maximal $L(u_i)$ by considering not only the implied faulty sets associated with the faulty units, but also the implied faulty sets associated with the nonfaulty units.

V. IMPLIED FAULTY SETS OF ALL UNITS: $\tau > 2$

As a result of the assumptions made in the previous section we saw that for the set of faulty units, F_S, Algorithm 1 generated a partition of at most two blocks. In this section we modify the assumptions on τ and k, consequently Algorithm 1 generates a partition of F_S of at most three blocks. Lemma 3 provides the proof when F_S has one block. Lemmas 7 and 8 below will prove the cases when F_S has two and three blocks, respectively. As these proofs are lengthy, they have been placed in the appendix. Theorem 4 uses these three results to prove a lower bound on the maximal $\|L(u_i)\|$ of all units. Finally, Lemma 6 and a new result, Lemma 9, show that this bound is a greatest lower bound.

Lemma 7: If S is τ-diagnosable, if $1 \leq \|F_S\| \leq \tau$, if $\tau > 2$, and if Algorithm 1 generates a two block partition $\{X_1,X_2\}$ of F_S, at least one unit u_i in S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $\|L(u_i)\| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$.

Lemma 8: If S is τ-diagnosable, if $\tau > 2$, if $1 \leq \|F_S\| \leq \tau$, and if Algorithm 1 generates a three block partition $\{X_1,X_2,X_3\}$ of F_S, at least one unit u_i in S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $\|L(u_i)\| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$.

The following theorem extends Theorem 3 by considering the implied faulty sets of both faulty and nonfaulty units.

Theorem 4: If S is τ-diagnosable, if $1 \leq |F_S| \leq \tau$, and if $\tau > 2$, at least one unit in S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$.

Proof: Suppose the system S satisfies the following assumptions:

(H1) S is τ-diagnosable,

(H2) $\tau > 2$,

(H3) $1 \leq |F_S| \leq \tau$,

(H4) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, and

(H5) $|L(u_i)| \leq \tau - k$ for all u_i in S, where k is the smallest integer such that $\tau \leq 7k + 2$.

The set of faulty units, F_S, is a critical subset of S. Algorithm 1 generates a partition $\{X_1, X_2, \ldots, X_p\}$ of F_S. Lemma 4 and (H5) imply that $|F_S| \geq p(2k + 1)$, where p is the number of blocks in the partition. In this case $|F_S| \leq \tau \leq 7k + 2$, thus $p \leq 4 - (k+2)/(2k+1)$, and the fact that $k \geq 1$ implies that $1 \leq p \leq 3$.

If $p = 1$, that is, if the partition of F_S has one block, then there exists a unit u_{1*} in F_S such that $G(u_{1*}) \cap F_S = F_S$. Lemma 3 implies that either $L(u_{1*}) \cap G(u_{1*}) \neq \phi$ or $|L(u_{1*})| \geq \tau + 1$, contradicting either (H4) or (H5). If the partition of F_S has two blocks, then Lemma 7 implies that assumptions (H1), (H2), (H3), (H4), and (H5) lead to a contradiction. Similarly, if the partition of F_S has three blocks, then Lemma 8 implies that the five assumptions lead to a contradiction.

Therefore, we may conclude that if S is τ-diagnosable, if $\tau > 2$,

and if $1 \leq |F_S| \leq \tau$, at least one unit in S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$. □

Theorems 2 and 4 show that the set of values of τ may be partitioned into intervals of length 7, except for the first interval of length 2. Thus, for a τ-diagnosable system in which $1 \leq |F_S| \leq \tau$ and $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, Theorem 2 implies that if $\tau \leq 2$, at least one unit u_i exists such that $|L(u_i)| \geq \tau + 1$, and Theorem 4 implies that if $\tau \leq 9$, at least one unit u_i exists such that $|L(u_i)| \geq \tau$, if $\tau \leq 16$, at least one unit u_i exists such that $|L(u_i)| \geq \tau - 1$, and so forth.

Lemma 6 shows that for $3 \leq \tau \leq 8$ the lower bound on the cardinality of the maximal implied faulty set given in Theorem 3 is the greatest lower bound. The next lemma proves a similar result for $\tau > 8$.

Lemma 9: To every integer $\tau > 8$ corresponds at least one τ-diagnosable system S that has τ faulty units and one syndrome such that:

(i) $L(u_i) \cap G(u_i) = \phi$ for every u_i in S,

(ii) $|L(u_i)| \leq \tau - k + 1$ for every u_i in S, where k is the smallest integer such that $\tau \leq 7k + 2$,

(iii) $|L(u_i)| = \tau - k + 1$ for at least one faulty unit u_i, and

(iv) $|L(u_i)| = \tau - k + 1$ for at least one nonfaulty unit u_i.

Proof: Choose a value of τ, $\tau > 8$, and let k be the smallest integer such that $\tau \leq 7k + 2$. Construct a system S that has the partition $\{A_1, A_2, B_1, B_2, X_1, X_2, X_3, X_4\}$ as shown in Figure 6. The cardinality of each

block is as follows: $|A_1| = \lfloor \tau/2 \rfloor - k + 1$, $|A_2| = \lceil \tau/2 \rceil - k$, $|B_1| = |B_2| = k$, $|X_1| = \lceil \tau/2 \rceil - k + 1$, $|X_2| = \lfloor \tau/2 \rfloor - k + 1$, and $|X_3| = |X_4| = k - 1$. The definitions of τ and k imply that each block in the partition is nonempty, except $X_3 = X_4 = \phi$ when $k = 1$, and S has cardinality $2\tau + 1$.

The tests are organized in the following manner: the units within each block are completely connected, that is, every unit in X_1 tests every other unit in X_1, every unit in B_2 tests every other unit in B_2, and so forth; the edges shown in Figure 6 indicate that every unit in the block at the tail of the edge tests every unit in the block at the head of the edge, for example, every unit in X_1 tests every unit in B_1 and vice versa, every unit in X_2 tests every unit in X_4, and so forth.

As in the proof of Lemma 5 we use Sullivan's approach [SUL84] to show that S is τ-diagnosable. This system is also symmetric, so we solve eight network flow problems, one for each block. Once again (omitting some of the details) each network has a maximum flow of $(\tau + 1/2)$, thus S is τ-diagnosable.

In the system S the set of nonfaulty units is

$$G_S = A_1 \cup A_2 \cup B_1 \cup B_2$$

and the set of faulty units is

$$F_S = X_1 \cup X_2 \cup X_3 \cup X_4 \ .$$

Note that $|F_S| = \tau$. Figure 6 shows a syndrome consistent with the set

of faulty units.

For the given syndrome the following table lists the implied nonfaulty set, the implied faulty set, and the cardinality of the implied faulty set for each unit in S.

u_i *in*	$G(u_i)$	$L(u_i)$	$\|L(u_i)\|$
X_1	$X_1 \cup X_3 \cup X_4$	$A_1 \cup A_2 \cup B_1$	$\tau - k + 1$
X_2	$X_2 \cup X_3 \cup X_4$	$A_1 \cup A_2 \cup B_2$	$\tau - k + 1$
X_3	X_3	A_1	$\lfloor\tau/2\rfloor - k + 1$
X_4	X_4	A_2	$\lceil\tau/2\rceil - k$
A_1	$A_1 \cup B_1 \cup B_2$	$X_1 \cup X_2 \cup X_3$	$\tau - k + 1$
A_2	$A_2 \cup B_1 \cup B_2$	$X_1 \cup X_2 \cup X_4$	$\tau - k + 1$
B_1	B_1	X_1	$\lceil\tau/2\rceil - k + 1$
B_2	B_2	X_2	$\lfloor\tau/2\rfloor - k + 1$

S is τ-diagnosable, $\tau > 8$, it has τ faulty units, and it has a syndrome such that

(i) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S,

(ii) $\|L(u_i)\| \leq \tau - k + 1$ for each unit u_i in S, where k is the smallest integer such that $\tau \leq 7k + 2$,

(iii) $\|L(u_i)\| = \tau - k + 1$ for at least one faulty unit u_i, and

(iv) $\|L(u_i)\| = \tau - k + 1$ for at least one nonfaulty unit u_i. □

VI. CONCLUSION

We have presented results concerning the properties of the implied faulty sets in the PMC system level fault model. Unlike previous work on implied faulty set properties, we made no assumptions on the structural properties of a system, only that the system was τ-diagnosable and had at most τ faulty units. The results are not only interesting in themselves, but also because of their implications in the diagnosis process.

Given a τ-diagnosable system S and the implied faulty and nonfaulty sets for each unit, we can identify the set $F_0 = \{u_i \mid L(u_i) \cap G(u_i) \neq \phi\}$. If S has at most τ faulty units, then $\|F_0\| \leq \tau$. In this case, removing from S the units in F_0 and all tests involving these units produces a reduced system $(S - F_0)$ that is $(\tau - \|F_0\|)$-diagnosable. The results of this paper outline the properties of the maximal implied faulty sets in the reduced system $(S - F_0)$. If $(\tau - \|F_0\|) \leq 2$, then the units with the maximal $\|L(u_i)\|$ are faulty. If $3 \leq (\tau - \|F_0\|) \leq 9$, then there exists at least one unit u_i such that $\|L(u_i)\| \geq \tau$. If $\|L(u_i)\| > \tau$, then u_i is obviously faulty. If u_i is nonfaulty and $\|L(u_i)\| = \tau$, then $L(u_i) = F_S$ and every edge in $S - (L(u_i) \cup G(u_i))$ is a 0-edge. On the other hand, if u_i is faulty and $\|L(u_i)\| = \tau$, then there must be at least one 1-edge in edge in $S - (L(u_i) \cup G(u_i))$ because S is τ-diagnosable. Thus, for $\tau \leq 9$, which covers many reasonable applications of this model, the results of this paper allow us to develop direct diagnosis algorithms and avoid the added complexity of transforming the diagnosis problem into a graph

support problem.

REFERENCES

[ALL75] F. J. Allan, T. Kameda, and S. Toida, An approach to the diagnosability analysis of a system, *IEEE Trans. Comput.*, vol. C-24, pp. 1040-1042, Oct. 1975.

[CHW81] K. Y. Chwa and S. L. Hakimi, On fault identification in diagnosable systems, *IEEE Trans. Comput.*, vol. C-30, pp. 414-422, June 1981.

[DAH84] A. T. Dahbura and G. M. Masson, An $O(n^{2.5})$ fault identification algorithm for diagnosable systems, *IEEE Trans. Comput.*, vol. C-33, pp. 486-492, June 1984.

[DAH85] A. T. Dahbura, G. M. Masson, and C.-L. Yang, Self-implicating structures for diagnosable systems, *IEEE Trans. Comput.*, vol. C-34, pp. 718-723, Aug. 1985.

[HAK74] S. L. Hakimi and A. T. Amin, Characterization of connection assignment of diagnosable systems, *IEEE Trans. Comput.*, vol. C-23, pp. 84-88, Jan. 1974.

[KAM75] T. Kameda, S. Toida, and F. J. Allan, A diagnosing algorithm for networks, *Inform. Contr.*, vol. 29, pp. 141-148, 1975.

[KEN84] M. A. Kennedy and G. G. L. Meyer, Structured diagnosability conditions for the PMC system level fault model, Rpt. JHU/EECS-84/12, 1984.

[MAD77] R. F. Madden, An algorithm for system diagnosis, Raunvisindastofnun Haskolans, Rpt. No. RH-77-6, 1977.

[MEY78] G. G. L. Meyer and G. M. Masson, An efficient fault diagnosis algorithm for symmetric multiple processor architectures, *IEEE Trans. Comput.*, vol. C-27, pp. 1059-1063, Nov. 1978.

[MEY81] G. G. L. Meyer, A fault diagnosis algorithm for asymmetric modular architectures, *IEEE Trans. Comput.*, vol. C-30, pp. 81-83, Jan. 1981.

[MEY83] G. G. L. Meyer, The PMC system level fault model: Maximality properties of the implied faulty sets, Rpt. JHU/EECS-83/03, 1983.

[PRE67] F. P. Preparata, G. Metze, and R. T. Chien, On the connection assignment problem of diagnosable systems, *IEEE Trans. on Electronic Comput.*, vol. EC-16, pp. 848-854, Dec. 1967.

[SUL84] G. Sullivan, A polynomial time algorithm for fault diagnosability, *Proceedings of the 25th Annual Symposium on the Foundations of Computer Science*, pp. 148-156, 1984.

APPENDIX

Proof of Lemma 7: Assume that the system S satisfies the following assumptions:

(H1) S is τ-diagnosable,

(H2) $\tau > 2$,

(H3) $1 \leqslant |F_S| \leqslant \tau$,

(H4) $L(u_i) \cup G(u_i) = \phi$ for all u_i in S,

(H5) $|L(u_i)| \leqslant \tau - k$ for all u_i in S, where k is the smallest integer such that $\tau \leqslant 7k + 2$, and

(H6) Algorithm 1 generates a partition $\{X_1, X_2\}$ of F_S.

If $\tau \leqslant 6k + 2$, Lemma 2 shows that there exists at least one faulty unit u_i such that $|L(u_i)| \geqslant \tau - k + 1$. Thus, we consider the case $\tau \geqslant 6k + 3$.

Beginning with the discussion of $((L(u_{1*}) \cap L(u_{2*})) \cap G_S)$, this proof follows the proof of Theorem 3 exactly. In the interest of brevity we do not restate this material and rejoin the proof at Eq. (7), that is

$$a + b_1 + b_2 \leqslant \tau - 3k - 1 + (x_2 - w_2) \ .$$

We know that $x_1 + x_2 \leqslant \tau$, $x_2 \leqslant x_1$, and $\tau \leqslant 7k + 2$, thus $x_2 \leqslant \lfloor \tau/2 \rfloor$ and $x_2 \leqslant 3k + 1 + \lfloor k/2 \rfloor$. Recall that if u_{1*} is in $L(u_{2*})$ then $W_2 \neq \phi$ and $\tilde{X}_2 \subseteq W_2 \subseteq X_2$. If so, then Lemma 4 and (H5) imply that $w_2 \geqslant |\tilde{X}_2| \geqslant 2k + 1$ and thus, $x_2 - w_2 \leqslant k + \lfloor k/2 \rfloor$. Substituting this last inequality into Eq. (7) produces

$$a + b_1 + b_2 \leq \tau - (k + \lceil k/2 \rceil + 1) < \tau + 1 \tag{9}$$

which contradicts Eq. (1). Therefore, if (H1) through (H6) are satisfied, then $W_1 = W_2 = \phi$ and there are no 1-edges between X_1 and X_2.

We now consider the nonfaulty units in the system. Recall that $A = (L(u_{1*}) \cap L(u_{2*})) \cap G_S$ and $|A| = a$. Since $W_1 = \phi$, Eq. (6) becomes

$$a \geq \tau + k + 1 - x_2 \tag{10}$$

thus

$$a \geq \lceil \tau/2 \rceil + k + 1 \tag{11}$$

and $A \neq \phi$. There are no tests from $(G_S - A)$ to A, otherwise these units would also belong to A. Assumption (H4) implies that there are no 0-edges from F_S to A, and thus, A is a critical subset of S. Applying Algorithm 1 to A produces a partition $\{A_1, A_2, \ldots, A_q\}$, $1 \leq q \leq a$. Lemma 4 and (H5) imply that $a \geq q(2k + 1)$, where q is the number of blocks in the partition of A. To determine an upper bound on the cardinality of A, combine Eqs. (1) and (4) to get $\tau + 1 \leq 2\tau - 2k - a$, and thus

$$a \leq \tau - 2k - 1 \leq 5k + 1 \tag{12}$$

since $\tau \leq 7k + 2$. The partition of A contains at most $q \leq 3 - (k+1)/(2k+1)$ blocks, both q and k are integers, and we may conclude that the partition of A consists of one or two blocks. We will prove that in both cases the assumptions (H1) through (H6) lead to a contradiction.

We first consider the case in which A has a two block partition

$\{A_1, A_2\}$. The one block case $A = \{A_1\}$ will follow from this one. If A has a partition of two blocks, then there exists a unit u_{a1} in A_1 and a unit u_{a2} in A_2 such that $G(u_{a1}) \cap A_1 = A_1$ and $G(u_{a2}) \cap A_2 = A_2$. Thus $L(u_i) \subseteq L(u_{a1})$ for all u_i in A_1 and $L(u_i) \subseteq L(u_{a2})$ for all u_i in A_2. (For the rest of this proof we denote cardinality of any subset of S using lower case notation, i.e. $|A_1| = a_1$.) The blocks A_1 and A_2 have the following properties: $a_2 \leq a_1$, $a_2 \leq \lfloor a/2 \rfloor$, and $a_i \geq 2k + 1$ for $i = 1$ and $i = 2$.

Returning now to the units in X_2, we combine Eqs. (12) and (6) to get $\tau - 2k + 1 \geq \tau + k + 1 - x_2$, and thus

$$x_2 \geq 3k + 2 \ . \tag{13}$$

Since $x_2 \leq x_1$ and $x_2 \leq \lfloor \tau/2 \rfloor$, we see that $6k + 4 \leq |F_S| \leq \tau$. Therefore, if $|F_S| \leq 6k + 3$ or if $\tau \leq 6k + 3$ assumptions (H1) through (H6) can not hold.

We are interested in the subsets $L(u_{a1}) \cap X_2$ and $L(u_{a2}) \cap X_2$. Let $\hat{X}_2 = X_2 - (L(u_{a1}) \cap L(u_{a2}))$. For i in $\{1,2\}$ let X_{2i} be a subset of $\hat{X}_2$ such that $X_{2i} \cap L(u_{ai}) = \phi$ and let B_{2i} be the units in B_2 implied faulty by at least one unit in X_{2i}. The units in $(X_{2i} \cup B_{2i})$ are tested at most by the units in $X_2 - X_{2i}$ and $A - A_i$. Assumption (H1) implies that

$$x_{2i} + b_{2i} + 2(x_2 - x_{2i} + a - a_i) \geq 2\tau + 1 \tag{14}$$

We substitute $b_{2i} \leq b_2$ and $2x_2 \leq 2\lfloor \tau/2 \rfloor \leq \tau$ into Eq. (14) to get

$$b_2 + 2a + \tau \geq 2\tau + 2a_i + x_{2i} + 1 \tag{15}$$

and we substitute Eq. (3), $2a_i \geq 2(2k+1)$, and $x_{2i} \geq 0$ into Eq. (15) to get $\tau - k + a \geq \tau + 4k + 3$, that is

$$a \geq 5k + 3 \tag{16}$$

which contradicts Eq. (12). Therefore, $X_{2i} = \phi$ for i in $\{1,2\}$ which implies that $\hat{X}_2 = \phi$ and thus $X_2 \subseteq (L(u_{a1}) \cap L(u_{a2}))$.

Now we turn our attention to the units in X_1 that are implied faulty by the units in A. Let $\hat{X}_1 = X_1 - (L(u_{a1}) \cap L(u_{a2}))$. Suppose there exists a subset X_α of $\hat{X}_1$ such that $X_\alpha \cap L(u_j) = \phi$ for all u_j in A. We use the implied nonfaulty set $G(u_{2*})$ to partition X_α. Let $X_{\alpha 1} = X_\alpha \cap G(u_{2*})$ and let $X_{\alpha 2} = X_\alpha - X_{\alpha 1}$. Since there are no tests from any unit in B_1 to any unit in $G(u_{2*}) \cap X_1$, the units in $X_{\alpha 1}$ are tested at most by the units in $(X_1 - X_{\alpha 1}) \cup X_2$. Assumption (H1) implies that

$$x_{\alpha 1} + 2(x_1 - x_{\alpha 1} + x_2) \geq 2\tau + 1 \ . \tag{17}$$

Substituting $x_1 + x_2 \leq \tau$ into Eq. (17) we obtain $2\tau - x_{\alpha 1} \geq 2\tau + 1$. This can not be true, thus $X_{\alpha 1} = \phi$ and $X_{\alpha 2} = X_\alpha$.

Let B_α be the units in B_1 implied faulty by at least one unit in X_α. The units in $X_\alpha \cup B_\alpha$ are tested at most by the units $X_1 - X_\alpha$, thus assumption (H1) implies that

$$x_\alpha + b_\alpha + 2(x_1 - x_\alpha) \geq 2\tau + 1 \ . \tag{18}$$

Note that $b_\alpha \leq b_1$ and $b_1 \leq \tau - k - a$ from Eq. (3). Substituting this, plus $2x_1 \leq 2\tau - 2x_2$ into Eq. (18) we get

$$\tau - k - a + 2\tau - x_\alpha \geq 2\tau + 1 + 2x_2$$

and therefore

$$\tau \geq a + 2x_2 + k + 1 + x_\alpha \ . \qquad (19)$$

Now substituting Eq. (10) into Eq. (19) we get

$$\tau \geq \tau + 2k + 2 + x_2 + x_\alpha \qquad (20)$$

which can not be true. Thus, if assumptions (H1) through (H6) hold then $\hat{X}_1 \subseteq (L(u_{a1}) \cup L(u_{a2}))$.

Partition $\hat{X}_1$ into four blocks, $\{X_{11}, X_{12}, X_{13}, X_{14}\}$ such that
(i) $(X_{11} \cup X_{12}) \subseteq L(u_{a1})$ and $(X_{11} \cup X_{12}) \cap L(u_{a2}) = \phi$,
(ii) $(X_{13} \cup X_{14}) \subseteq L(u_{a2})$ and $(X_{13} \cup X_{14}) \cap L(u_{a1}) = \phi$,
(iii) $(X_{11} \cup X_{13}) \cap G(u_{2*}) = \phi$, and
(iv) $(X_{12} \cup X_{14}) \subseteq G(u_{2*})$.

Therefore, $\hat{x}_1 = x_{11} + x_{12} + x_{13} + x_{14}$. The above definitions, plus the fact that $X_2 \subseteq (L(u_{a1}) \cap L(u_{a2}))$, imply that $\|L(u_{a1})\| \geq x_1 + x_2 - (x_{13} + x_{14})$ and $\|L(u_{a2})\| \geq x_1 + x_2 - (x_{11} + x_{12})$. Since $\|L(u_i)\| \leq \tau - k$ for all u_i in S observe that

$$x_{13} + x_{14} \geq x_1 + x_2 + k - \tau \qquad (21)$$

and

$$x_{11} + x_{12} \geq x_1 + x_2 + k - \tau \ . \qquad (22)$$

We now show that if all the assumptions are satisfied, then $X_{11} = X_{13} = \phi$. Let B_{11} be the units in B_1 implied faulty by at least

one unit in X_{11} and let B_{13} be the units in B_1 implied faulty by at least one unit in X_{13}. There are no tests from X_2 to either X_{11} or X_{13}.

The units in $X_{11} \cup B_{11}$ are tested at most by the units in $X_1 - \hat{X}_1$ and A_1, thus (H1) implies that

$$x_{11} + b_{11} + 2(x_1 - \hat{x}_1 + a_1) \geq 2\tau + 1 . \tag{23}$$

From Eqs. (21) and (22) we see that $x_{11} - 2\hat{x}_1 \leq 3\tau - 3(x_1 + x_2 + k)$. Substituting this, plus $b_{11} \leq b_1$ and $2a_1 = 2a - 2a_2$ into Eq. (23) and we get

$$(b_1 + 2a - 2a_2) + 2x_1 + 3\tau - 3(x_1 + x_2 + k) \geq 2\tau + 1$$

and therefore

$$b_1 + 2a + \tau \geq x_1 + 3x_2 + 2a_2 + 3k + 1 . \tag{24}$$

Substituting Eqs. (2) and (12) into the left hand side of Eq. (24), substituting $x_1 + 3x_2 \geq 4x_2 \geq 4(3k + 2)$ and $2a_2 \geq 2(2k + 1)$ into the right hand side of Eq. (24) we obtain

$$\tau - k + (\tau - 2k - 1) + \tau \geq 19k + 11 \tag{25}$$

which reduces to $3\tau \geq 22k + 12$, that is, $\tau \geq 7k + 4 + (k/3)$. This contradicts assumption (H5), thus $X_{11} = \phi$.

The units in $X_{13} \cup B_{13}$ are tested at most by the units in $X_1 - \hat{X}_1$ and A_2, thus (H1) implies that

$$x_{13} + b_{13} + 2(x_1 - \hat{x}_1 + a_2) \geq 2\tau + 1 . \tag{26}$$

From Eqs. (21) and (22) we see that $x_{13} - 2\hat{x}_1 \le 3\tau - 3(x_1 + x_2 + k)$. Substituting this, plus $b_{13} \le b_1$ and $2a_2 \le a$ into Eq. (26) we get

$$b_1 + a + 2x_1 + 3\tau - 3(x_1 + x_2 + k) \ge 2\tau + 1$$

and

$$b_1 + a + \tau \ge x_1 + 3x_2 + 3k + 1 \ . \qquad (27)$$

Substituting Eq. (2) into the left hand side of Eq. (27) and substituting $x_1 + 3x_2 \ge 4x_2 \ge 4(3k + 2)$ into the right hand side of Eq. (27) we obtain

$$(\tau - k) + \tau \ge 15k + 9 \qquad (28)$$

which reduces to $2\tau \ge 16k + 9$, and $\tau \ge 8k + (9/2)$. This contradicts assumption (H5), thus $X_{13} = \phi$.

As a result of the partitioning algorithm, $|L(u_{2*}) \cap F_S| \le |L(u_{1*}) \cap F_S| = x_1$. We know that $|L(u_{2*}) \cap F_S| \ge x_2 + x_{12} + x_{14}$, thus, $x_1 - x_{14} \ge x_2 + x_{12} \ge x_2$. This implies that $|L(u_{a1})| \ge x_1 + x_2 - x_{14} \ge 2x_2$. Substituting $x_2 \ge 3k + 2$ and $7k + 2 \ge \tau$ into this last inequality produces $|L(u_{a1})| \ge 6k + 4 \ge \tau - k + 2$, which contradicts (H5). Therefore, if Algorithm 1 generates a two block partition of A, assumptions (H1), (H2), (H3), (H4), (H5), and (H6) lead to a contradiction.

Now consider the case in which Algorithm 1 generates a one block partition of A. In this case there exists a unit u_{a1} in A such that $G(u_{a1}) \cap A = A$ and $L(u_j) \subseteq L(u_{a1})$ for all u_j in A. Let

$\hat{X}_2 = X_2 - L(u_{a1})$. From the previous case we see that if (H1) through (H6) are satisfied, then $\hat{X}_2 = \phi$ and $X_2 \subseteq L(u_{a1})$. Suppose now that there exists a subset $\hat{X}_1$ of X_1 such that $\hat{X}_1 = X_1 - L(u_{a1})$. Once again the previous case indicates that if the six assumptions hold, then $\hat{X}_1 = \phi$. Thus, $\|L(u_{a1})\| \geq x_1 + x_2 \geq 6k + 4 \geq \tau - k + 2$, which contradicts (H5). Therefore, if Algorithm 1 generates a one block partition of A, the assumptions (H1), (H2), (H3), (H4), (H5), and (H6) can not hold simultaneously.

We have shown that in all cases the assumptions (H1) through (H6) lead to a contradiction. Therefore, if S is τ-diagnosable, if $\tau > 2$, if $1 \leq \|F_S\| \leq \tau$, and if Algorithm 1 generates a two block partition $\{X_1, X_2\}$ of F_S, then there exists at least one unit u_i in S such that either $L(u_i) \cap G(u_i) = \phi$ or $\|L(u_i)\| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$. □

Proof of Lemma 8: Suppose the system S satisfies the following assumptions:

(H1) S is τ-diagnosable,

(H2) $\tau > 2$,

(H3) $1 \leq \|F_S\| \leq \tau$,

(H4) $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, and

(H5) $\|L(u_i)\| \leq \tau - k$ for all u_i in S, where k is the smallest integer such that $\tau \leq 7k + 2$.

(H6) Algorithm 1 generates a three block partition $\{X_1, X_2, X_3\}$ of F_S.

Once again we denote all subsets of S using upper case letters and the

cardinalities of these subsets using lower case letters.

If $\tau \leq 6k + 2$, Lemma 1 implies that there exists at least one faulty unit u_i such that $|L(u_i)| \geq \tau - k + 1$, and thus we consider the case $6k + 3 \leq \tau \leq 7k + 2$. The partition $\{X_1, X_2, X_3\}$ of F_S has the properties $x_1 + x_2 + x_3 \leq \tau$ and $x_1 \geq x_2 \geq x_3$. Lemma 4 and assumption (H5) imply that $x_i \geq 2k + 1$ for i in $\{1,2,3\}$, thus $|F_S| \geq 6k + 3$ and

$$2k + 1 \leq x_3 \leq \lfloor \tau/3 \rfloor \tag{29}$$

$$2k + 1 \leq x_2 \leq \left\lfloor (\tau - x_3)/2 \right\rfloor \leq (\tau - 2k - 1)/2 \tag{30}$$

$$\tau/3 \leq x_1 \leq \tau - (x_1 + x_2) \leq 3k\ . \tag{31}$$

There exists a unit u_{1*} in X_1 such that $G(u_{1*}) \cap X_1 = X_1$, a unit u_{2*} in X_2 such that $G(u_{2*}) \cap X_2 = X_2$, and a unit u_{3*} in X_3 such that $G(u_{3*}) \cap X_3 = X_3$. Therefore, $L(u_j) \subset L(u_{i*})$ for all u_j in X_i, i in $\{1,2,3\}$. We partition the nonfaulty units using the implied faulty sets $L(u_{1*})$, $L(u_{2*})$, and $L(u_{3*})$. Let

$$A = (L(u_{1*}) \cap L(u_{2*}) \cap L(u_{3*})) \cap G_S\ ,$$

$$B_1 = (L(u_{1*}) \cap L(u_{2*})) \cap (G_S - A)\ ,$$

$$B_2 = (L(u_{2*}) \cap L(u_{3*})) \cap (G_S - A)\ ,$$

$$B_3 = (L(u_{3*}) \cap L(u_{1*})) \cap (G_S - A)\ ,$$

$$B = B_1 \cup B_2 \cup B_3,$$

$$C_1 = L(u_{1*}) \cap (G_S - (A \cup B)) ,$$

$$C_2 = L(u_{2*}) \cap (G_S - (A \cup B)) ,$$

$$C_3 = L(u_{3*}) \cap (G_S - (A \cup B)) .$$

$$C = C_1 \cup C_2 \cup C_3,$$

and finally, let

$$Z = F_S \cup A \cup B \cup C.$$

The set $S - Z$ contains only nonfaulty units, and as in the proof of Theorem 3, there are no tests from $S - Z$ to Z. Thus, Z itself must be τ-diagnosable, $z \geq 2\tau + 1$, and

$$a + b + c \geq \tau + 1 \tag{32}$$

since $x_1 + x_2 + x_3 \leq \tau$.

We now consider $L(u_{i*}) \cap F_S$ for i in $\{1,2,3\}$. Assumption (H4) states that $L(u_i) \cap G(u_i) = \phi$ for all u_i in S, so there are no 1-edges between units in a block X_i. There may, however, be 1-edges between units in different blocks of F_S. Define the sets W_i, i in $\{1,2,3,4,5,6\}$, as follows: $W_1 = L(u_{1*}) \cap X_2$, $W_2 = L(u_{1*}) \cap X_3$, $W_3 = L(u_{2*}) \cap X_1$, $W_4 = L(u_{2*}) \cap X_3$, $W_5 = L(u_{3*}) \cap X_1$, and $W_6 = L(u_{3*}) \cap X_2$. Let $W = \bigcup_{i=1}^{6} W_i$, and let $|W| = w = \sum_{i=1}^{6} w_i$. For i,j in $\{1,2,3\}$, if u_{j*} is in $L(u_{i*})$ then u_{i*} is in $L(u_{j*})$, $\tilde{X}_j \subset L(u_{i*})$, and $\tilde{X}_i \subset L(u_{j*})$. If $W_i \neq \phi$,

Lemma 4 and (H5) imply that $w_i \geq 2k + 1$.

By assumption (H5) $|L(u_i)| \leq \tau - k$ for all u_i in S, thus

$$|L(u_{1*})| = a + b_1 + b_3 + c_1 + w_1 + w_2 \leq \tau - k \ , \tag{33}$$

$$|L(u_{2*})| = a + b_1 + b_2 + c_2 + w_3 + w_4 \leq \tau - k \ , \tag{34}$$

$$|L(u_{3*})| = a + b_2 + b_3 + c_3 + w_5 + w_6 \leq \tau - k \ . \tag{35}$$

Combining Eqs. (33), (34), and (35) we get

$$3a + 2b + c + w \leq 3\tau - 3k \ . \tag{36}$$

Since S is τ-diagnosable, we can combine Eqs. (32) and Eq. (36) to get

$$a + b \leq 2\tau - (a + w + 3k + 1) \ . \tag{37}$$

To get an upper bound for $(a + b + c)$, we need an upper bound for c. Let X_{1c} be those units in X_1 implied faulty by the units in C_1. The units in $X_{1c} \cup C_1$ are tested only by the units in A, B_1, B_3, W_1, and W_2. Thus, assumption (H1) implies that

$$x_{1c} + c_1 + 2(a + b_1 + b_3 + w_1 + w_2) \geq 2\tau + 1 \ . \tag{38}$$

Substituting Eq. (33) and $x_{1c} \leq x_1$ into Eq. (38) we get
$x_1 + c_1 + 2(\tau - k - c_1) \geq 2\tau + 1$ and

$$x_1 - 2k - 1 \geq c_1 \ . \tag{39}$$

Using a similar approach we can show that

$$x_2 - 2k - 1 \geq c_2, \tag{40}$$

and

$$x_3 - 2k - 1 \geq c_3 , \tag{41}$$

and thus

$$c \leq x_1 + x_2 + x_3 - (6k + 3) \leq k - 1 \tag{42}$$

since $x_1 + x_2 + x_3 \leq \tau \leq 7k + 2$. Combining Eqs. (37) and (42) we get

$$a + b + c \leq 2\tau - (a + w + 2k + 2) . \tag{43}$$

Depending on the syndrome any of the following statements may be true:

(S1) u_{1*} *is in* $L(u_{2*})$ and u_{2*} *is in* $L(u_{1*})$,

(S2) u_{1*} *is in* $L(u_{3*})$ and u_{3*} *is in* $L(u_{1*})$,

(S3) u_{2*} *is in* $L(u_{3*})$ and u_{3*} *is in* $L(u_{2*})$.

If at least two of {(S1),(S2),(S3)} are true then at least four of $\{W_1,W_2,W_3,W_4,W_5,W_6\}$ are nonempty and $w \geq 4(2k + 1) \geq \tau + k + 2$. In this case Eq. (43) becomes

$$a + b + c \leq 2\tau - (a + \tau + 3k + 4) \leq \tau - (a + 3k + 4) , \tag{44}$$

which contradicts Eq. (32). Thus, if S is τ-diagnosable at most one of {(S1),(S2),(S3)} is true.

We now show that if at most one of {(S1),(S2),(S3)} is true then $A \neq \phi$. Suppose not, then the units in B_1 are tested only by faulty

units. Any test from X_3 to B_1 that has a 1 outcome implies that $L(u_{3*}) \cap B_1 \neq \phi$ and any such test with a 0 outcome implies that both u_{1*} and u_{2*} are in $L(u_{3*})$. So there are no tests from X_3 to B_1 and B_1 is tested only by the units in $X_1 \cup X_2$. Assumption (H1) implies that

$$b_1 + 2(x_1 + x_2) \geq 2\tau + 1 . \tag{45}$$

Substitute $2(x_1 + x_2) \leq 2\tau - 2x_3$ into Eq. (45) we get

$$b_1 \geq 2x_3 + 1 . \tag{46}$$

Using similar reasoning we can show that

$$b_2 \geq 2x_1 + 1 \tag{47}$$

and

$$b_3 \geq 2x_2 + 1 . \tag{48}$$

Both B_1 and B_3 are in $L(u_{1*})$ so we can combine Eqs. (46) and (48) with Eq. (33) to get

$$\tau - k \geq b_1 + b_3 \geq 2x_2 + 2x_3 + 2 . \tag{49}$$

Note that Eqs. (29) and (30) imply that $2x_2 + 2x_3 \geq 4(2k + 1)$, thus Eq. (49) becomes $\tau \geq 9k + 6$, which contradicts assumption (H5). Thus, if $A = \phi$, either $B_1 = \phi$ or $B_3 = \phi$. We can also show that Eqs. (34), (46), and (47) imply that either $B_1 = \phi$ or $B_2 = \phi$ and Eqs. (35), (47), and (48) imply that either $B_2 = \phi$ or $B_3 = \phi$. Therefore, if $A = \phi$ at most one of $\{B_1, B_2, B_3\}$ is nonempty.

For i in $\{1,2,3\}$, recall that $\tilde{X}_i$ is the subset of X_i containing u_{i*} and all units that are implied faulty if u_{i*} is implied faulty. If $B_2 \neq \phi$ and $B_1 = B_3 = \phi$, the units in $\tilde{X}_1 \cup C_1$ are tested at most by the units in $W_1 \cup W_2$. In this case (H1) implies that

$$\tilde{x}_1 + c_1 + 2(w_1 + w_2) \geq 2\tau + 1 \ . \tag{50}$$

Substituting $\tilde{x}_1 \leq x_1$ and Eq. (33) into Eq. (50) we get $x_1 + (\tau - k) + w_1 + w_2 \geq 2\tau + 1$ or

$$x_1 + w_1 + w_2 \geq \tau + k + 1 \ . \tag{51}$$

At most one of $\{(S1),(S2),(S3)\}$ is true, so at most one of $\{W_1,W_2\}$ is nonempty. Therefore, $w_1 + w_2 \leq \max\{w_1,w_2\} \leq x_2$ and Eq. (51) becomes

$$\tau + k + 1 \leq x_1 + x_2 \leq \tau - x_3 \tag{52}$$

which is obviously a contradiction. Similar contradictions arise when either $B_1 \neq \phi$ or $B_3 \neq \phi$. We conclude that if assumptions (H1), (H2), (H3), (H4), (H5) and (H6) are satisfied and at most one of $\{(S1),(S2),(S3)\}$ is true, then $A \neq \phi$.

Since $A = ((L(u_{1*}) \cap L(u_{2*}) \cap L(u_{3*})) \cap G_S)$, we see that $(\tilde{X}_1 \cup \tilde{X}_2 \cup \tilde{X}_3) \subset L(u_j)$ for all u_j in A. Lemma 4 and assumption (H5) imply that $|\tilde{X}_i| \geq 2k + 1$ for i in $\{1,2,3\}$. Therefore, $|L(u_j)| \geq 6k + 3 \geq \tau - k + 1$ for all u_j in A, which contradicts (H5).

Thus, in all cases the assumptions (H1) through (H6) lead to a contradiction. Therefore, if S is τ-diagnosable, if $\tau \geq 2$, if $1 \leq |F_S| \leq \tau$, and if Algorithm 1 generates a three block partition

$\{X_1, X_2, X_3\}$ of F_S, at least one unit u_i in S exists such that either $L(u_i) \cap G(u_i) \neq \phi$ or $|L(u_i)| \geq \tau - k + 1$, where k is the smallest integer such that $\tau \leq 7k + 2$. □

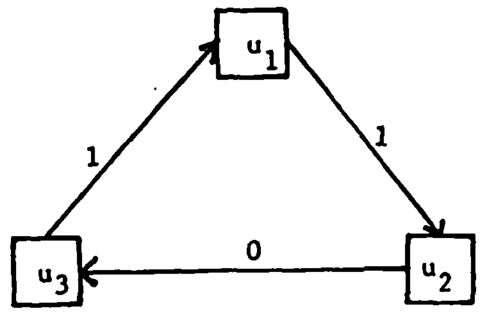


Figure 1: A 1-diagnosable system (Lemma 1)

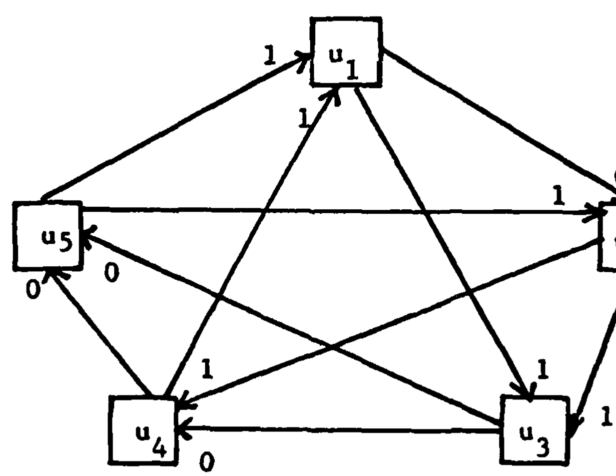


Figure 2: A 2-diagnosable system (Lemma 1)

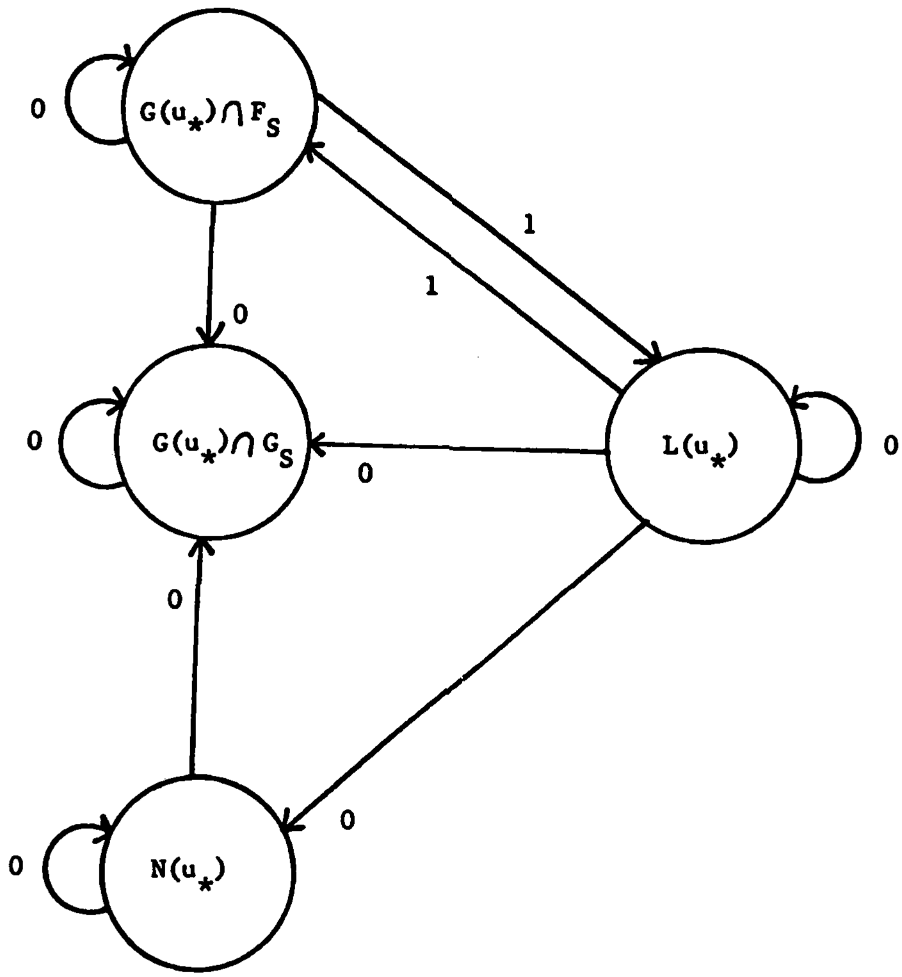


Figure 3: A consistent partition (Lemma 3)

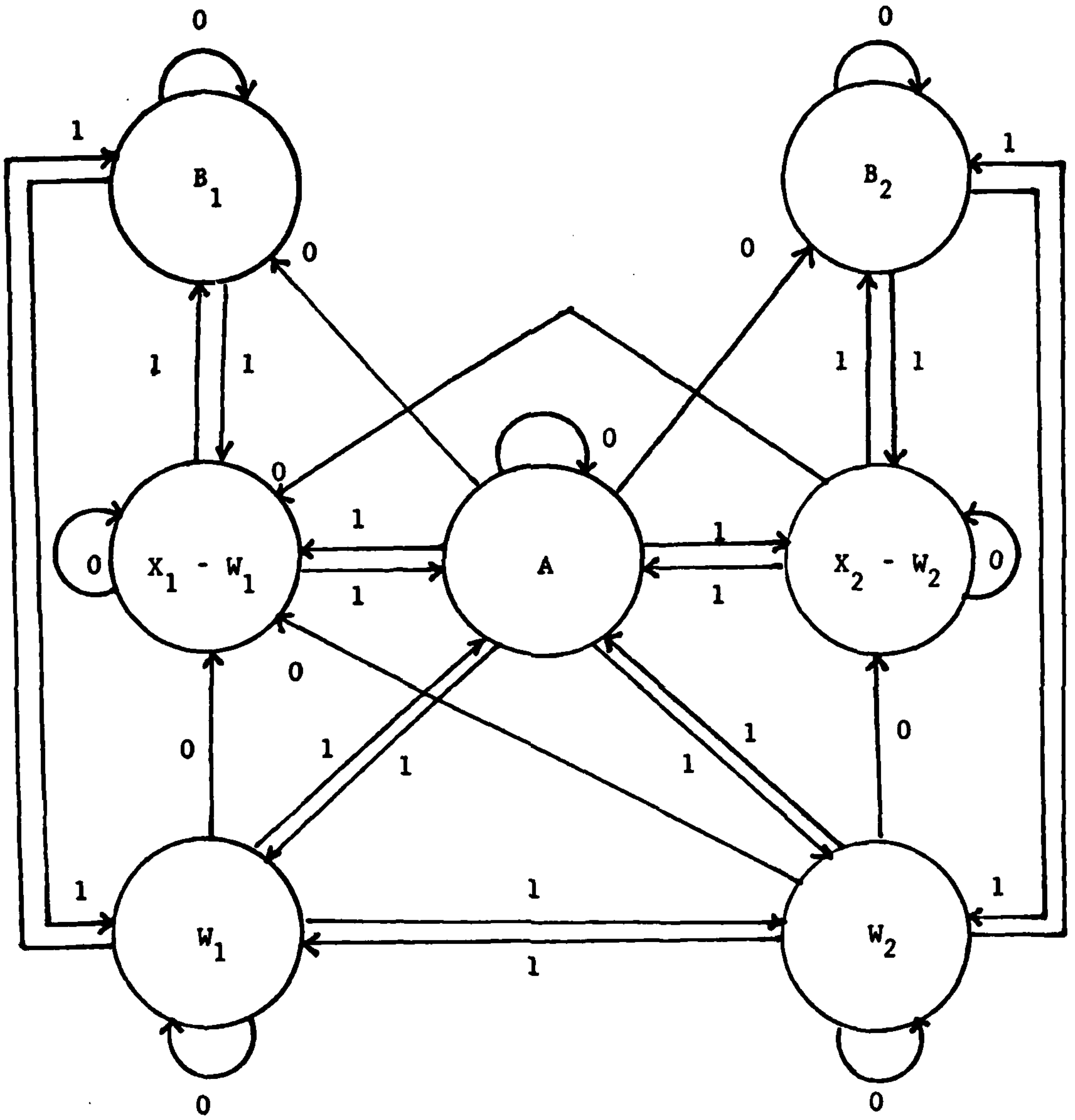


Figure 4: The system Z (Lemma 5)

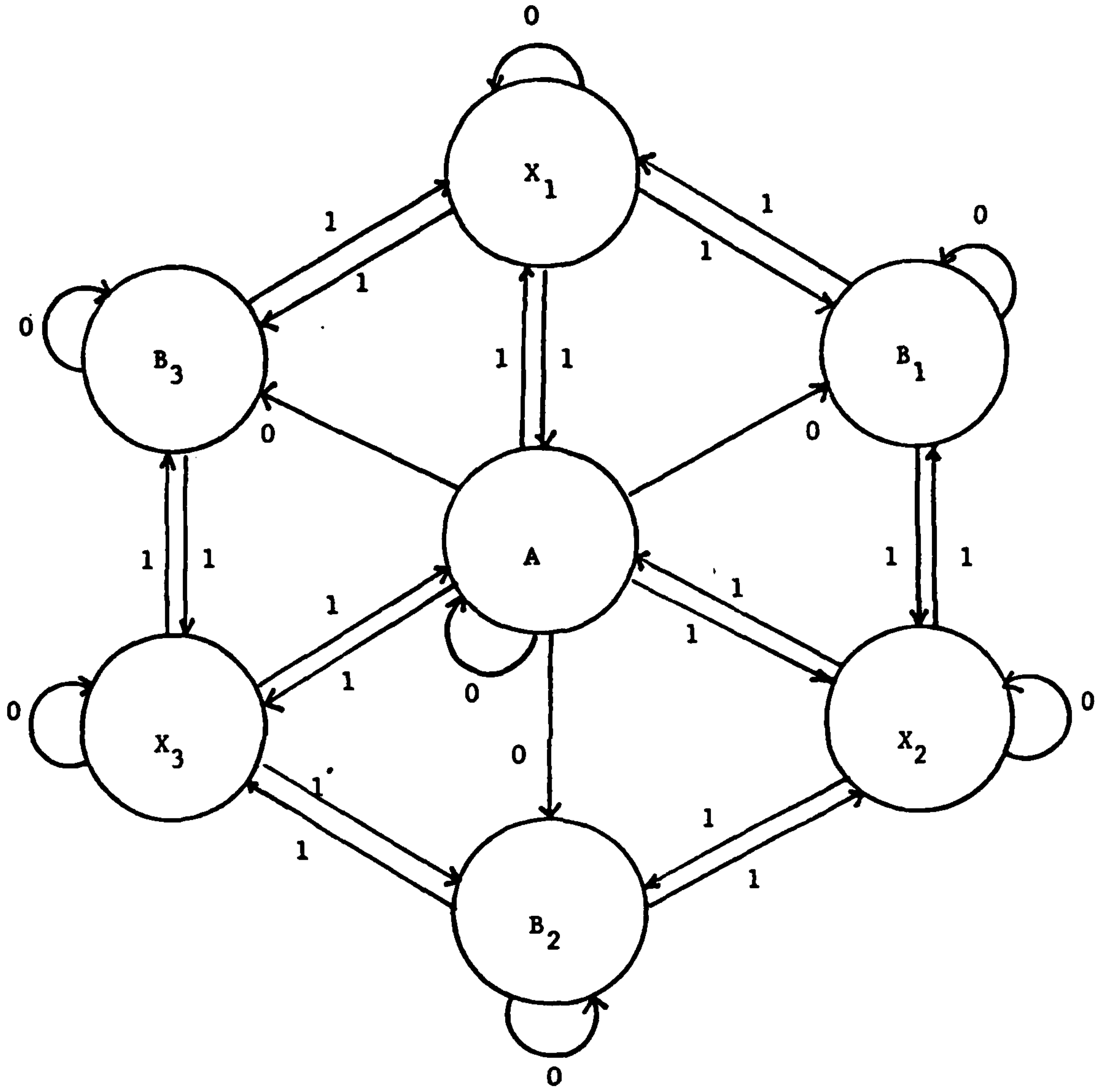


Figure 5: A τ-diagnosable system (Lemma 6)

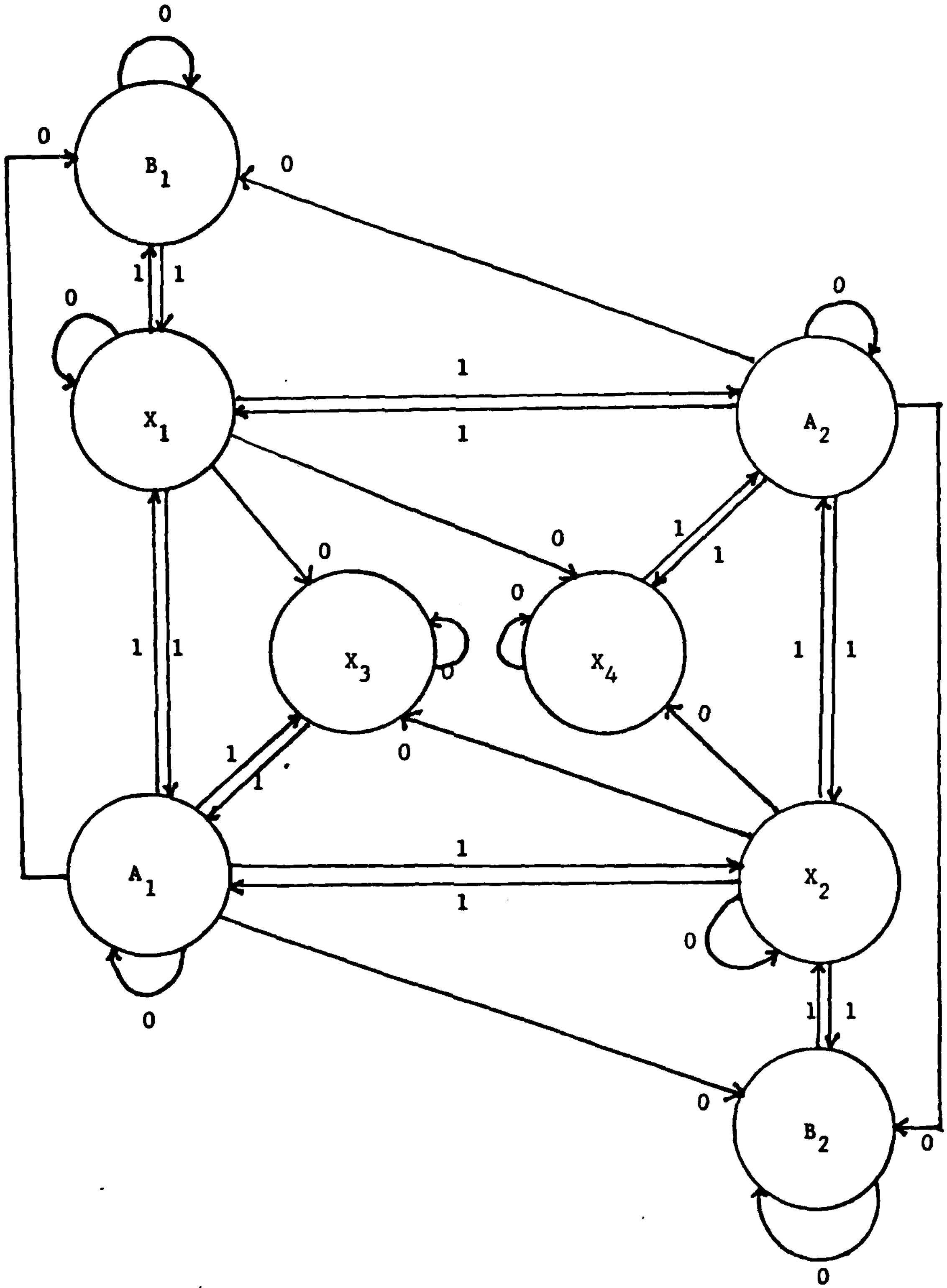


Figure 6: A $\mathcal{T}$-diagnosable system (Lemma 9)

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

AD-A172190

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Unrestricted. This document has been approved for public release and sale; its distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): JHU/EECS-86/09	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION: The Johns Hopkins University; 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION: Air Force Office of Scientific Research /NM
6c. ADDRESS (City, State and ZIP Code): Charles and 34th Streets, Baltimore, Maryland 21218	7b. ADDRESS (City, State and ZIP Code): Bolling AFB, Washington DC 20332
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: AFOSR/PKZ; 8b. OFFICE SYMBOL (If applicable): N/A	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: AFOSR-85-0097
8c. ADDRESS (City, State and ZIP Code): Building 410, Bolling AFB - DC 20332-6448	10. SOURCE OF FUNDING NOS.: PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.

11. TITLE (Include Security Classification) THE PMC SYSTEM LEVEL FAULT MODEL: CARDINALITY PROPERTIES OF THE IMPLIED FAULTY SETS (Unclassified)

12. PERSONAL AUTHOR(S) Kennedy, M.A. and Meyer, G.G.L.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Interim	FROM 1/1/86 TO 9/1/86	September 5, 1986	52

16. SUPPLEMENTARY NOTATION

N/A

17. COSATI CODES		
FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

System level fault model, faults, tests, test outcome, implied faulty set, diagnosis algorithms.

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

In this report we consider one aspect of the PMC system level fault model, the properties of the implied faulty sets. For τ-diagnosable systems that have at most faulty units we present lower bounds on the cardinality of the maximal implied faulty sets. When $\tau \leq 2$, we show that the cardinality of the maximal implied faulty sets is greater than τ. In the case $\tau > 2$ we have two results: (i) the cardinality of the maximal implied faulty sets associated with the faulty units is greater than or equal to $\tau - k + 1$, where k is the smallest integer such that $\tau \leq 6k + 2$, and (ii) the cardinality of the maximal implied faulty sets of all the units is greater than or equal to $\tau - k + 1$, where now k is the smallest integer such that $\tau \leq 7k + 2$. Finally, we show that these bounds are greatest lower bounds and in the conclusion indicate how these results may be used in diagnosis algorithms.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT: UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION: Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL: Dr. Marc Q. Jacobs	22b. TELEPHONE NUMBER (Include Area Code): (202)-767-4940; 22c. OFFICE SYMBOL

DD FORM 1473, 83 APR   EDITION OF 1 JAN 73 IS OBSOLETE.

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

END

10-86

DTIC